L-14

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
8. Februar 2001 (08.02.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/10077 A1

(51) Internationale Patentklassifikation[7]: H04L 9/06

(21) Internationales Aktenzeichen: PCT/DE00/02518

(22) Internationales Anmeldedatum: 31. Juli 2000 (31.07.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 36 529.6 3. August 1999 (03.08.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **ORGA KARTENSYSTEME GMBH** [DE/DE]; Am Hoppenhof 33, D-33104 Paderborn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: **JAHNICH, Michael** [DE/DE]; Am Rippinger Weg 15, D-33098 Paderborn (DE).

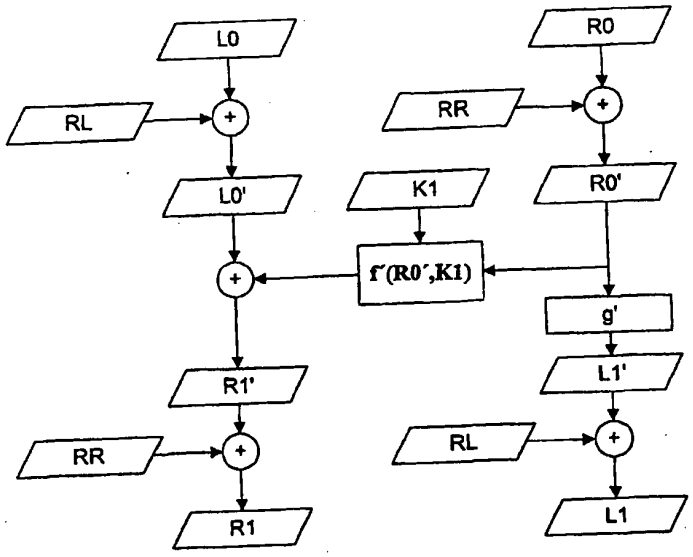
(81) Bestimmungsstaaten *(national)*: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW.

(84) Bestimmungsstaaten *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR EXECUTING AN ENCRYPTION PROGRAM IN A MICROPROCESSOR-ASSISTED, PORTABLE DATA CARRIER

(54) Bezeichnung: VERFAHREN ZUR AUSFÜHRUNG EINES VERSCHLÜSSELUNGSPROGRAMMS IN EINEM MIKROPROZESSORGESTÜTZTEN, TRAGBAREN DATENTRÄGER



(57) Abstract: The invention relates to a method, in which the data to be encrypted is linked by a random number using an exclusive-OR operation prior to encryption. According to the invention, the encryption program is modified in such a way that the standard encryption text can be ultimately retrieved. The inventive method provides protection against the DPA (Differential Power Analysis) attack.

[Fortsetzung auf der nächsten Seite]

WO 01/10077 A1

FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *Mit internationalem Recherchenbericht.*
— *Vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Die Erfindung beschreibt ein Verfahren, bei dem die zu verschlüsselnden Daten mit einer Zufallszahl vor der Verschlüsselung über eine XOR-Operation verknüpft werden. Dabei wird das Verschlüsselungsprogramm derart modifiziert, daß letztendlich wieder der Standard-Verschlüsselungstext erhalten wird. Das erfindungsgemäße Verfahren ist eine Maßnahme gegen den sogenannten DPA-Angriff.

Titel:

VERFAHREN ZUR AUSFÜHRUNG EINES VERSCHLÜSSELUNGSPROGRAMMS IN EINEM MIKROPROZESSORGESTÜTZTEN, TRAGBAREN DATENTRÄGER

Die Erfindung bezieht sich auf ein Verfahren zur Ausführung eines Verschlüsselungsprogramms zur Verschlüsselung von Daten in einem mikroprozessorgestützten, tragbaren Datenträger. Ein derartiger tragbarer Datenträger ist beispielsweise eine Chipkarte, die zum Datenaustausch und zur Energieversorgung mit einem entsprechenden Kartenterminal, dem Datenaustauschgerät, verbunden wird. Mikroprozessorchipkarten, die in der Lage sind, anhand eines Verschlüsselungsprogramms Daten zu verschlüsseln, werden beispielsweise in Form von Bankkarten oder in Form von Zugangsberechtigungskarten zu Mobilfunknetzen nach dem GSM-Standard eingesetzt. Der Verschlüsselung von Daten und Informationen kommt dabei eine immer größere Bedeutung zu. Dementsprechend steigen auch die Anforderungen an die Sicherheit der Verschlüsselung gegenüber Angriffen.

Die tragbaren Datenträger, die Gegenstand der vorliegenden Erfindung sind, verfügen nicht über eine eigene Energieversorgung, beispielsweise in Form einer Batterie oder Solarzelle. Die Energieversorgung des tragbaren Datenträgers erfolgt durch das Datenaustauschgerät, mit dem dann auch die Kommunikation stattfindet. Chipkarten weisen auf der Kartenoberfläche elektrische Kontaktflächen auf, um über korrespondierende Kontakte im Datenaustauschgerät mit diesem kommunizieren zu können. Eine dieser Kontaktflächen ist für die Zuführung der Versorgungsspannung und des Versorgungsstroms vorgesehen. Eine andere Kontaktfläche dient dem Masseanschluß, eine der seriellen, bidirektionalen Datenübertragung vom und zum Datenaustauschgerät, eine der Zuführung eines Taktsignals, eine weitere Kontaktfläche ist für den Empfang eines Reset-Signals vorgesehen.

Die tragbaren Datenträger, die Gegenstand der Erfindung sind, weisen einen integrierten Halbleiterbaustein auf, in dem ein Mikroprozessor mit einem Festwertspeicher (ROM- Read Only Memory), einem flüchtigen Arbeitsspeicher (RAM- Random Access Memory), in den

das Betriebssystem oder zumindest Teile davon abgelegt sind, und einem nichtflüchtigen, änderbaren Speicher (EEPROM - Electrical Eraseable Programmable Read Only Memory) auf. Damit stellt der tragbare Datenträger eine Mikrorechnereinheit dar, die jedoch einer externen (von außerhalb des tragbaren Datenträgers) Spannungs- und Stromversorgung Bedarf.

Der Mikroprozessor bildet die Verarbeitungsschaltungen zur Ausführung von Programmen, insbesondere auch von Verschlüsselungsprogrammen, die im EEPROM-Speicher und/oder ROM-Speicher gespeichert sind. Hier sind ebenfalls geheime Schlüssel von außen nicht zugänglich abgespeichert. Diese Schlüssel dienen der Verschlüsselung der Daten. Da die Verschlüsselungsprogramme (Algorithmen) an sich meistens bekannt sind, liegt die ganze Sicherheit hinsichtlich der Verschlüsselung der Daten bei den geheimen Schlüsseln. Die verschlüsselten Daten sind demnach eine Funktion des Verschlüsselungsprogramms in Abhängigkeit von den unverschlüsselten Daten (Klartext) und wenigstens einem geheimen Schlüssel:

Ein derartiges, allgemein bekanntes Verschlüsselungsprogramm ist beispielsweise der sogenannte DES-Algorithmus. Beim DES-Algorithmus beruht die Verschlüsselung zumindest teilweise darauf, daß die zu verschlüsselnden Klartextdaten direkt oder in modifizierter Form durch eine Substitutionsoperation ersetzt werden. Dabei gilt:

$$D_{encrypt} = VP\ (D, K_i)$$

wobei

D die Eingangsdaten für die Substitutionsoperation

K_i einen geheimen Schlüssel

und $D_{encrypt}$ das Ergebnis der Substitutionsoperation bezeichnet,

Aufgrund des physikalischen Aufbaus und der physikalischen Eigenschaften der in den tragbaren Datenträgern eingesetzten Halbleiterchips ist die Strom- bzw. Leistungsaufnahme des tragbaren Datenträgers während der Ausführung von Programmen nicht konstant, sondern vielmehr zeitlichen Schwankungen unterworfen. Dabei hat es sich gezeigt, daß die Schwankungen des Versorgungsstroms sogar zu bestimmten Programmkommandos, insbesondere Substitutionsoperationen, und zur binären Struktur (Zahl der Nullen und Einsen) der zu verarbeitenden (verschlüsselnden) Daten korreliert. Unter Umständen erfolgen die Schwankungen sogar synchron zum Takt mit dem der tragbare Datenträger betrieben wird.

Für einen mit der Technik vertrauten, unbefugten Benutzer ist es ein leichtes diese Schwankungen des Versorgungsstromes, der vom Datenaustauschgerät an den tragbaren Datenträger geliefert wird, mittels eines Speicher-Oszilloskops aufzuzeichnen, indem er in die Versorgungsstromleitung einen Meßwiderstand einbaut und den Spannungsabfall an diesem auf dem Oszilloskop aufzeichnet. Mit Blick auf die Ausführung von Verschlüsselungsprogrammen in tragbaren Datenträgern ergibt sich hiermit für Angreifer die Möglichkeit über die Aufzeichnung der Stromschwankungen beim Ausführen des Verschlüsselungsprogramms Rückschlüsse auf die verwendeten geheimen Schlüssel und/oder die zu verschlüsselnden Daten zu ziehen. Dies wird insbesondere dadurch erleichtert, daß die Verschlüsselungsprogramme an sich bekannt sind. Dem Angreifer kommt dabei zugute, daß es eine Korrelation zwischen den Stromschwankungen und einer sogenannten Entscheidungsfunktion gibt, wobei die Ausgangswerte der Entscheidungsfunktion von den zu verschlüsselnden Daten als Input und dem geheimen Schlüssel abhängen. Die Entscheidungsfunktion wird so bezeichnet, da anhand der Korrelation dieser Funktion mit dem Stromverlauf die entscheidende Aussage über den richtigen Schlüssel getroffen werden kann. Zeichnet ein Angreifer nun für eine Vielzahl von Verschlüsselungen mit jeweils unterschiedlichen - ihm jedoch bekannten - Daten jeweils die Stromschwankungen auf, so kann er aus Unterschieden in den jeweiligen Stromschwankungscharakteristika durch Korrelation mit den zuvor berechneten Entscheidungsfunktionen Rückschlüsse auf den verwendeten Schlüssel ziehen. Hierbei kann ein Angreifer auf aus der Mathematik bekannte statistische Analysemittel und Korrelationsverfahren zurückgreifen. Hat der Angreifer auf diese Weise den geheimen Schlüssel herausgefunden, so ist die Sicherheit der Verschlüsselung nicht mehr gewährleistet, da die Verschlüsselungsprogramme an sich bekannt sind. Insbesondere bei symmetrischen Verschlüsselungsverfahren, wo zur Ver- und Entschlüsselung ein und derselbe Schlüssel verwendet wird, wäre der Angreifer dann in der Lage, verschlüsselte Daten zu entschlüsseln.

Ein derartiger Angriff auf die Sicherheit von tragbaren Datenträgern wird als Differential Power Analysis (DPA) bezeichnet. Zur Lösung dieses Problems wird in der C2-Intern, Edition Nr. 67, vom 15.7.98 (Kopie ist als Anhang zum Patentantrag beigefügt) vorgeschlagen, in den tragbaren Datenträger eine zusätzliche elektronische Schaltung einzubringen, die die Stromschwankungen kompensieren soll, so daß ein Angreifer diese nicht mehr feststellen kann und daraus keine Rückschlüsse mehr ziehen kann.

Diese Lösung ist jedoch sehr aufwendig und teuer, da sie die Implementierung eines zusätzlichen elektronischen Bauteils erfordert. Da jedoch insbesondere der Chipkartenmarkt ein Massenmarkt ist, ist hier der Preisdruck besonders hoch, so daß eine derart aufwendige und teuere Lösung nicht akzeptabel ist.

Aufgabe der Erfindung ist es daher, tragbare Datenträger der oben genannten Art gegenüber einem Angriff auf die Sicherheit bei der Datenverschlüsselung in effektiver, einfacher und kostengünstiger Weise sicherer zu machen.

Diese Aufgabe wird erfindungsgemäß dadurch gelöst, daß die Eingangsdaten **D** vor der Verschlüsselung über eine XOR-Operation (⊕) mit einer Zufallszahl **R** verknüpft werden, wobei das Ergebnis dieser XOR-Operation als modifizierte Eingangsdaten D´für ein unter Einbeziehung der Zufallszahl **R** zumindest hinsichtlich der Substitutionsoperation modifiziertes Verschlüsselungsprogramm **VP´**dienen, dabei gilt

$$D' = (D \oplus R)$$

und

$$D'_{encrypt} = VP'(D', K_i)$$

Das Ergebnis $D'_{encrypt}$ des modifizierten Verschlüsselungsprogramms **VP´** wird nun wiederum mit der Zufallszahl **R** über XOR-Operation verknüpft wird, um wieder $D_{encrypt}$ zu liefern, dabei gilt:

$$D_{encrypt} = D'_{encrypt} \oplus R$$

Aufgrund der XOR-Verknüpfung der Eingangsdaten mit einer Zufallszahl korrelieren die Stromschwankungen im Verlauf des Verschlüsselungsprogramms, insbesondere im Verlauf von Substitutionsoperationen, nicht mehr mit den dem Angreifer bekannten Eingangsdaten. Der oben beschriebene DPA-Angriff wird somit erfolgreich abgewehrt. Durch das erfindungsgemäße Verfahren werden die Daten, die in den Substitutionsoperationen des DES-Algorithmus verarbeitet werden, von den Eingangsdaten, die dem Angreifer bekannt sind, in nicht nachvollziehbarer Weise entkoppelt. Dabei entsprechen die Ausgangsdaten des DES-Algorithmus aber wieder dem „korrekten" DES-Ergebnis.

Anhand der beigefügten Zeichnungen soll die Erfindung nachfolgend näher erläutert werden. Es zeigt:

Figur 1 eine Versuchsanordnung zur Aufzeichnung von Stromschwankungen bei der Ausführung von Verschlüsselungsprogrammen,

Figur 2 ein Beispiel für den zeitlichen Verlauf des Versorgungsstroms während der Ausführung des Verschlüsselungsprogramms,

Figur 3 ein Flußdiagramm für den kompletten Ablauf des DES-Algorithmus,

Figur 4 ein Flußdiagramm für den Ablauf einer DES-Runde,

Figur 5 ein Flußdiagramm für den Ablauf vor und nach der 1. DES-Runde

Figur 6 +7 Flußdiagramme wie in Fig.5 , jedoch mit einer zusätzlichen XOR-Verknüpfung.

In Figur 1 ist ein tragbarer Datenträger in Form einer Mikroprozessor-Chipkarte gezeigt. Der integrierte Halbleiterbaustein mit dem Mikroprozessor und den Speichern (RAM, ROM, EEPROM) befindet sich in einem Chipmodul, das als separates Bauteil in den Kartenkörper eingesetzt wird. Auf dem Chipmodul befinden sich die elektrischen Kontaktflächen zum Datenaustausch und zur Energieversorgung in Verbindung mit dem Datenaustauschgerät (in dem dargestellten Fall ist dies ein Kartenterminal). Aus Gründen der Übersichtlichkeit ist nur die Strom- und Spannungsversorgungsleitung vom Kartenterminal an die entsprechende Kontaktfläche der Karte sowie die Masseleitung eingezeichnet. Für den vorstehend beschriebenen DPA-Angriff auf die Chipkarte, wird in die Stromversorgungsleitung ein Meßwiderstand (z.B. ein 1 Ω) eingebaut und über den Spannungsabfall an diesem Widerstand indirekt die Stromschwankungen gemessen und in einem Speicheroszilloskop aufgezeichnet.

Wie man in Fig. 2 erkennen kann sind die Stromschwankungsamplituden, die während der Ausführung eines Verschlüsselungsprogramms auftreten können, stellenweise ein Vielfaches der mittleren Stromaufnahme (Gleichstromanteil), dabei liegen die Stromwerte im Bereich von Milliampere. Ein Angreifer könnte nun das Verschlüsselungsprogramm in der Chipkarte mehrfach jeweils mit verschiedenen Daten, die ihm bekannt sind, ausführen lassen und dabei jeweils die Stromschwankungen und die Verschlüsselungsresultate aufzeichnen. Parallel dazu kann der Angreifer nun für dieselben Daten Entscheidungsfunktionen berechnen, deren Werte von den Daten und von einem Schlüsselwert abhängen, und mittels mathematischer

Analysemethoden versuchen, herauszufinden, ob es Korrelationen zwischen den Stomaufzeichnungen und den berechneten Entscheidungsfunktionen gibt.

In Figur 3 ist das Flußdiagramm für den Ablauf des DES-Algorithmus (Data Encryption Standard) aufgezeichnet. Zu Details des DES-Algorithmus sei auf das Buch „Applied Cryptography" von Bruce Schneider verwiesen, das im John Wiley & Sons Verlag erschienen ist. Beim DES-Algorithmus werden die zu verschlüsselnden Daten blockweise in Form von 64 Bit langen Datenblocks (Plaintext) verschlüsselt. Dabei wird der zu verschlüsselnde Datenblock zuerst einer sogenannten IP-Operation (Initial Permutation) unterzogen, die eine Vertauschung der Bits gemäß einer Permutationstabelle bewirkt. Anschließend wird Datenblock in zwei jeweils 32 Bit lange Hälften (L0 und R0) aufgeteilt. Dann beginnen 16 Runden mit identischen Operationen (gekennzeichnet durch die Funktion *f*), wo die Daten mit dem bzw. den geheimen Schlüsseln (K1 bis K16) verschlüsselt werden. Bei der Funktion *f* handelt es sich um eine nichtlineare Funktion. Für die jeweils nächste Runde leiteten sich die linke und die rechte Datenhälfte wie folgt ab:

$L_i = R_{i-1}$

$R_i = L_{i-1}$ XOR $f(R_{i-1}, K_i)$.

Zum Schluß werden die Ergebnisse (L16, R16) der letzten DES-Runde wieder zu einem 64 Bit Datenblock zusammengefügt und dieser Datenblock der inversen IP-Operation (IP^{-1}) unterzogen. Das Endergebnis ist dann der verschlüsselte Datenblock (Chipertext).

Erfindungsgemäß wird nun der zu verschlüsselnde Datenblock vor der Initial Permutation Operation mit einer Zufallszahl (R) über eine XOR-Operation verknüpft. Diese Zufallszahl besteht ihrerseits aus zwei jeweils 32 Bit langen Hälften (RL und RR). Nach der inversen Initial Permutation Operation wird der Datenblock dann wieder mit der Zufallszahl (R)über eine XOR-Operation verknüpft, um den „korrekten" Chipertext gemäß Standard zu liefern. Dabei wird die linke Hälfte des Datenblocks mit der linken Hälfte (RL) der Zufallszahl (R) - der linke Zufallszahl-Datenblock - über eine XOR-Operation verknüpft und die rechte Hälfte des Datenblocks mit der rechten Hälfte (RR) der Zufallszahl (R) - der rechte Zufallszahl-Datenblock - über eine XOR-Operation verknüpft.

In Figur 4 ist eine Runde des DES-Algorithmus dargestellt. Jede Runde beginnt mit einer sogenannte Key-Transformation, wobei die Bits des Schlüssels (Key, K) zyklisch vertauscht („Shift-Operation") werden und anschließend über eine sogenannte Permuted-Choice-Operation 48 Bits als eigentlicher Schlüssel für eine nachfolgende XOR-Operation extrahiert werden. Bestandteil jeder DES-Runde ist ferner eine sogenannte Expansion-Permutation-Operation, bei der die rechte Datenblockhälfte (R_i) vertauscht und von 32 Bit auf 48 Bit expandieret wird. Das Ergebnis dieser Expansion-Permutation-Operation wird nun über eine XOR-Operation mit dem geheimen (transformierten) Schlüssel verknüpft und durch eine Substitutionsoperation durch Werte einer definierten Substitutionstabelle (sog. S-Box) ersetzt und anschließend permutiert. Die vorstehend beschriebenen Operationen bilden die eigentlichen Grundfunktionen und werden in der Funktion *f* zusammengefaßt

In Figur 5 ist der erfindungsgemäß modifizierte Ablauf für die 1.DES-Runde dargestellt.

Die rechte Datenhälfte (R0) wird über eine XOR-Operation mit der rechten Hälfte (RR) der Zufallszahl verknüpft, um die modifizierte rechte Datenhälfte (R0′) zu liefern.
Es gilt: $R0' = RR \oplus R0$.
Die linke Datenhälfte (L0) wird über eine XOR-Operation mit der linken Hälfte (RL) der Zufallszahl verknüpft, um die modifizierte linke Datenhälfte (L0′) zu liefern.
Es gilt: $L0' = RL \oplus L0$.

Durch diese zufällige XOR-Verknüpfung werden die tatsächlich zu verschlüsselnden Daten, die dem Angreifer bekannt sind, von den Daten, die in den DES-Runden verarbeitet werden so entkoppelt, daß keine Korrelation mehr besteht zwischen den Eingangsdaten, die dem Angreifer bekannt sind, und dem Stromverlauf während der Ausführung der DES-Runden.

R0′dient nun als Eingang für eine erfindungsgemäß modifizierte DES-Runde (gekennzeichnet durch *f*′) , deren Ergebnis dann R1′ ist. Es gilt: $R1' = L0' \oplus f'(R0', K1)$.
K1 ist dabei der geheime Schlüssel für die 1.DES-Runde (bzw. die Transformation des Schlüssels).

Um nun einen standardgemäß verschlüsselten Text (R1) gemäß DES zu erhalten, wird R1´über eine XOR-Operation mit der rechten Hälfte (RR) der Zufallszahl (R) verknüpft. Es gilt: $R1 = RR \oplus R1'$.

Analog dazu wird R0´ über eine Funktion g' in eine Datenblockhälfte L1´ transformiert, die die Eigenschaft hat über eine XOR-Verknüpfung mit der linken Hälfte (RL) der Zufallszahl (R) in einen standardgemäß verschlüsselten Text (L1) gemäß DES umgewandelt zu werden. Die Funktion g', führt hierzu eine XOR-Verknüpfung von R0´mit einer Größe $R^+ = (RR \oplus RL)$ durch. Diese Transformation findet jeweils zwischen einzelnen DES-Runden statt, so daß allgemein gilt: $L'_{i+1} = R^+ \oplus R'_i$

Die standardgemäß verschlüsselten Texte (L1, R1) bilden den sogenannten Chipertext, der von dem berechtigten Empfänger der verschlüsselten Daten durch den an sich bekannten DES-Algorithmus bei Kenntnis des geheimen Schlüssels entschlüsselt werden kann. Dabei besteht allerdings in vorteilhafter Weise keine von außen nachvollziehbare Korrelation zwischen den zu verschlüsselnden Daten und den Daten, die in den DES-Runden verarbeitet werden. Durch diese Maßnahme wird das Ausspionieren des geheimen Schlüssels vereitelt.

Um am Ende wieder den standardgemäßen Chipertext liefern zu können, wird weiterhin die Substitutionsoperation S durch eine geänderte Substitutionsoperation S´ersetzt, indem die der Substitutionsoperation zugrunde liegenden Substitutionstabellen (sogenannte S-Boxen) modifiziert werden. Dies geschieht über eine XOR-Verknüpfung der Standard S-Boxen mit der oben erwähnten Größe R^+. Dabei gilt : $S' = P^{-1}(R^+) \oplus S$.

Dabei bezeichnet P^{-1} die inverse Permutationsoperation nach der Substitutionsoperation (siehe Figur 4).

In einer Ausführungsform der Erfindung wird im Verlauf des Verschlüsselungsprogramms mindestens eine Datenblockhälfte L'_i mit einer weiteren Zufallszahl RX über eine XOR-Operation verknüpft: $L''_i = RX \oplus L'_i$ (siehe Figur 6). Zur Neutralisation dieser XOR-Verknüpfung wird jeweils in jeder zweiten weiteren DES-Runde die jeweils andere Datenblockhälfte R'_i mit der Zufallszahl RX über eine XOR-Operation vor der Ausführung der Funktion *f* verknüpft (siehe Figur 7). Durch diese Maßnahme der zusätzlichen zufälligen XOR-Verknüpfung wird eine weiteres Maß an Sicherheit gewonnen.

Patentansprüche

1. Verfahren zur Ausführung eines Standard-Verschlüsselungsprogramms (z.B. des DES-Algorithmus) zur Verschlüsselung von Daten in einem mikroprozessorgestützten, tragbaren Datenträger, der zum Datenaustausch und zur Energieversorgung mit einem Datenaustauschgerät verbunden wird, wobei die Verschlüsselung zumindest teilweise darauf beruht, daß die zu verschlüsselnden Klartextdaten direkt oder in modifizierter Form durch eine Substitutionsoperation durch Werte einer definierten Substitutionstabelle ersetzt werden, dabei gilt:

$$D_{encrypt} = VP\ (D, K_i)$$

wobei

VP das Verschlüsselungsprogramm

D die Eingangsdaten für das Verschlüsselungsprogramm

K_i einen geheimen Schlüssel für die Verschlüsselung

und $D_{encrypt}$ das Ergebnis des Verschlüsselungsprogramms bezeichnet,

dadurch gekennzeichnet, daß

- die Eingangsdaten **D** vor der Verschlüsselung über eine XOR-Operation (⊕) mit einer Zufallszahl **R** verknüpft werden, wobei das Ergebnis dieser XOR-Operation als modifizierte Eingangsdaten D'für ein unter Einbeziehung der Zufallszahl **R** zumindest hinsichtlich der Substitutionsoperation modifiziertes Verschlüsselungsprogramm **VP'**dienen, dabei gilt

$$D' = (D \oplus R)$$

und

$$D'_{encrypt} = VP'\ (D', K_i)$$

- das Ergebnis $D'_{encrypt}$ des modifizierten Verschlüsselungsprogramms **VP'** mit der Zufallszahl **R** über XOR-Operation verknüpft wird, um wieder $D_{encrypt}$ zu liefern, dabei gilt:

$$D_{encrypt} = D'_{encrypt} \oplus R$$

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, daß
die Zufallszahl in einem Zufallszahlengenerator des tragbaren Datenträgers erzeugt wird.

3. Verfahren nach Anspruch 2,
dadurch gekennzeichnet, daß
der Zufallszahlengenerator als Programm in dem tragbaren Datenträger implementiert ist.

4. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, daß
die Zufallszahl von dem Datenaustauschgerät an den tragbaren Datenträger übermittelt wird.

5. Verfahren nach einem der vorstehenden Ansprüche, wobei der Verschlüsselungs-Algorithmus der DES-Algorithmus ist und somit die Verschlüsselung blockweise in Form Datenblocks erfolgt und ein Datenblock in eine linke und eine rechte Datenblockhälfte (L_i, R_i) von jeweils gleicher Länge aufgeteilt wird,

dadurch gekennzeichnet, daß

- die Zufallszahl (R) aus zwei gleich langen Datenblöcken (RL, RR) besteht, wobei der Zufallszahl-Datenblock (RL) zur XOR-Verknüpfung der linken Datenblockhälfte (L_i) und der Zufallszahl-Datenblock (RR) zur XOR-Verknüpfung der rechten Datenblockhälfte (R_i) vor der Inititial-Permutation-Operation verwendet wird,
- eine Größe R^+ berechnet wird, die gleich dem Ergebnis der XOR-Verknüpfung des rechten Zufallszahl-Datenblocks (RR) mit dem linken Zufallszahl-Datenblocks (RL) ist: $R^+ = (RR \oplus RL)$,
- die Standard-Substitutionsoperation S durch eine modifizierte Substitutionsoperation $S' = P^{-1}(R^+) \oplus S$ ersetzt wird, wobei $P^{-1}(R^+)$ die Anwendung der inversen Permutation-Operation auf die Größe R^+ bezeichnet,
- zwischen einzelnen DES-Runden zumindest eine Datenblockhälfte (R'_i) über eine XOR-Verknüpfung mit R^+ in eine andere Datenblockhälfte (L'_{i+1}) transformiert wird: $L'_{i+1} = R^+ \oplus R'_i$
- nach Beendigung der DES-Runden
  die linke Hälfte des nach der inversen Initial-Permutation-Operation erhaltenen Datenblocks mit dem linken Zufallszahl-Datenblock (RL) über eine XOR-Operation verknüpft wird,
  und die rechte Hälfte des nach der inversen Initial-Permutation-Operation erhaltenen Datenblocks mit dem rechten Zufallszahl-Datenblock (RL) über eine XOR-Operation verknüpft wird,
  um schließlich wieder einen verschlüsselten Datenblock gemäß Standard-DES zu erhalten.

6) Verfahren nach Anspruch 5,
dadurch gekennzeichnet, daß

- in der ersten DES-Runde mindestens eine Datenblockhälfte L'_i mit einer weiteren Zufallszahl RX über eine XOR-Operation verknüpft wird: $L''_i = RX \oplus L'_i$
- jeweils in jeder zweiten weiteren DES-Runde die jeweils andere Datenblockhälfte R'_i mit der Zufallszahl RX über eine XOR-Operation vor der Ausführung der Funktion *f* verknüpft wird.

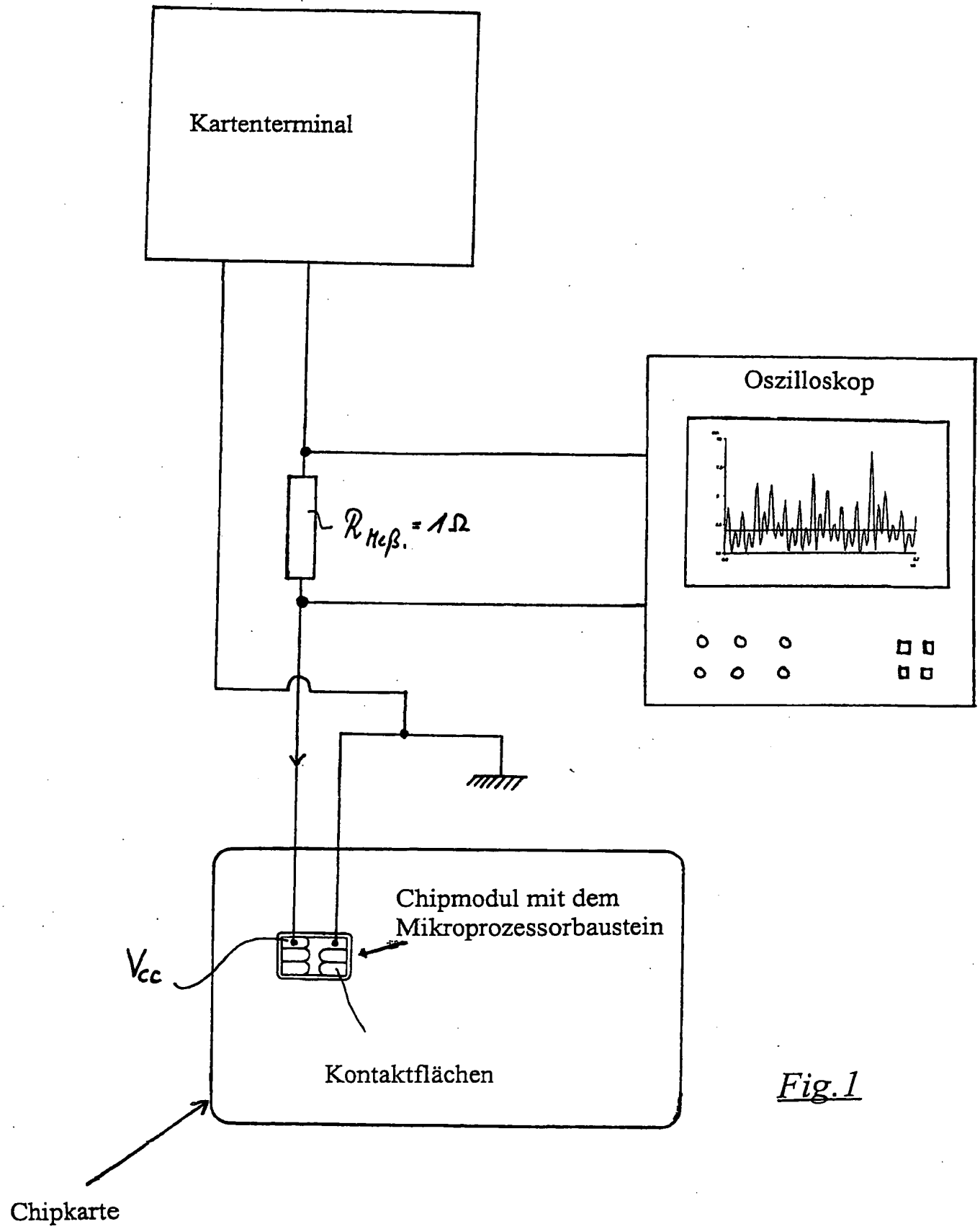

Kartenterminal
Oszilloskop
$R_{Meß.} = 1\Omega$
Chipmodul mit dem
Mikroprozessorbaustein
V_{CC}
Kontaktflächen
Chipkarte

Fig.1

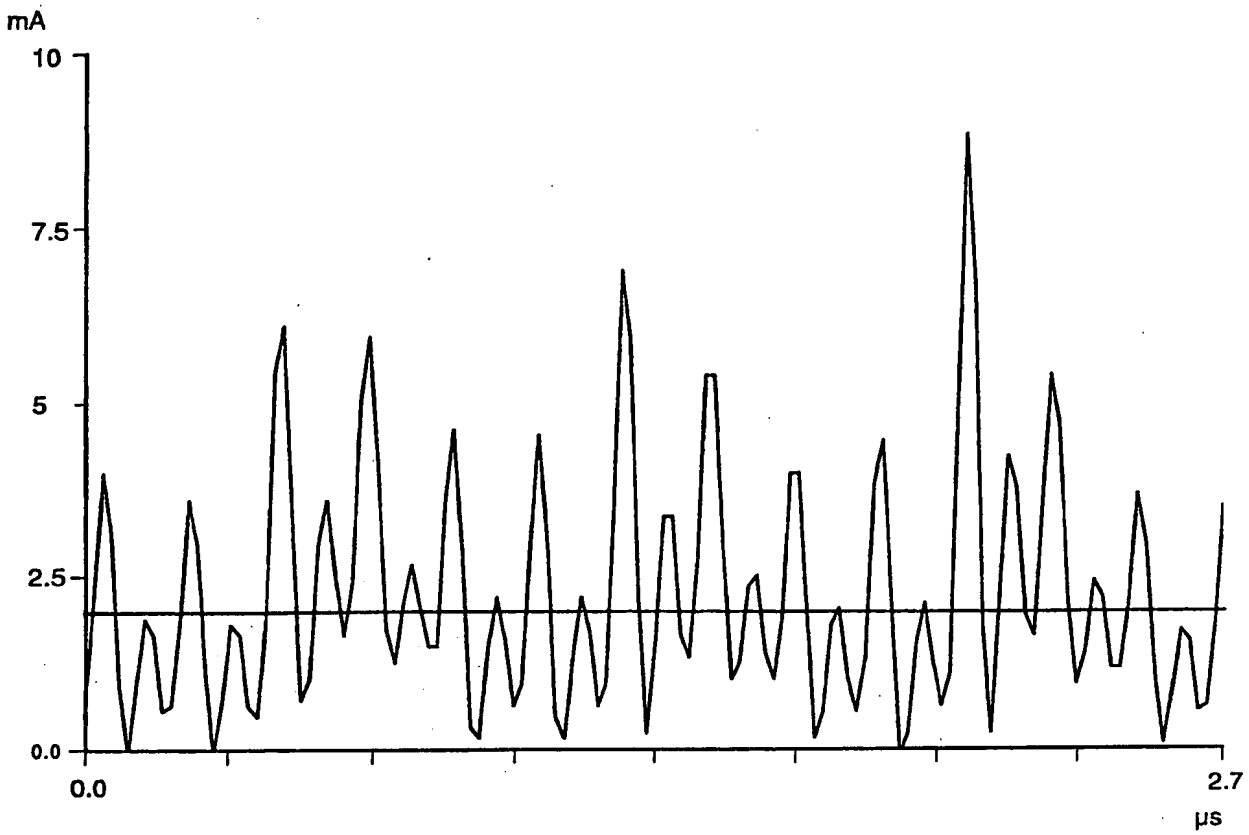
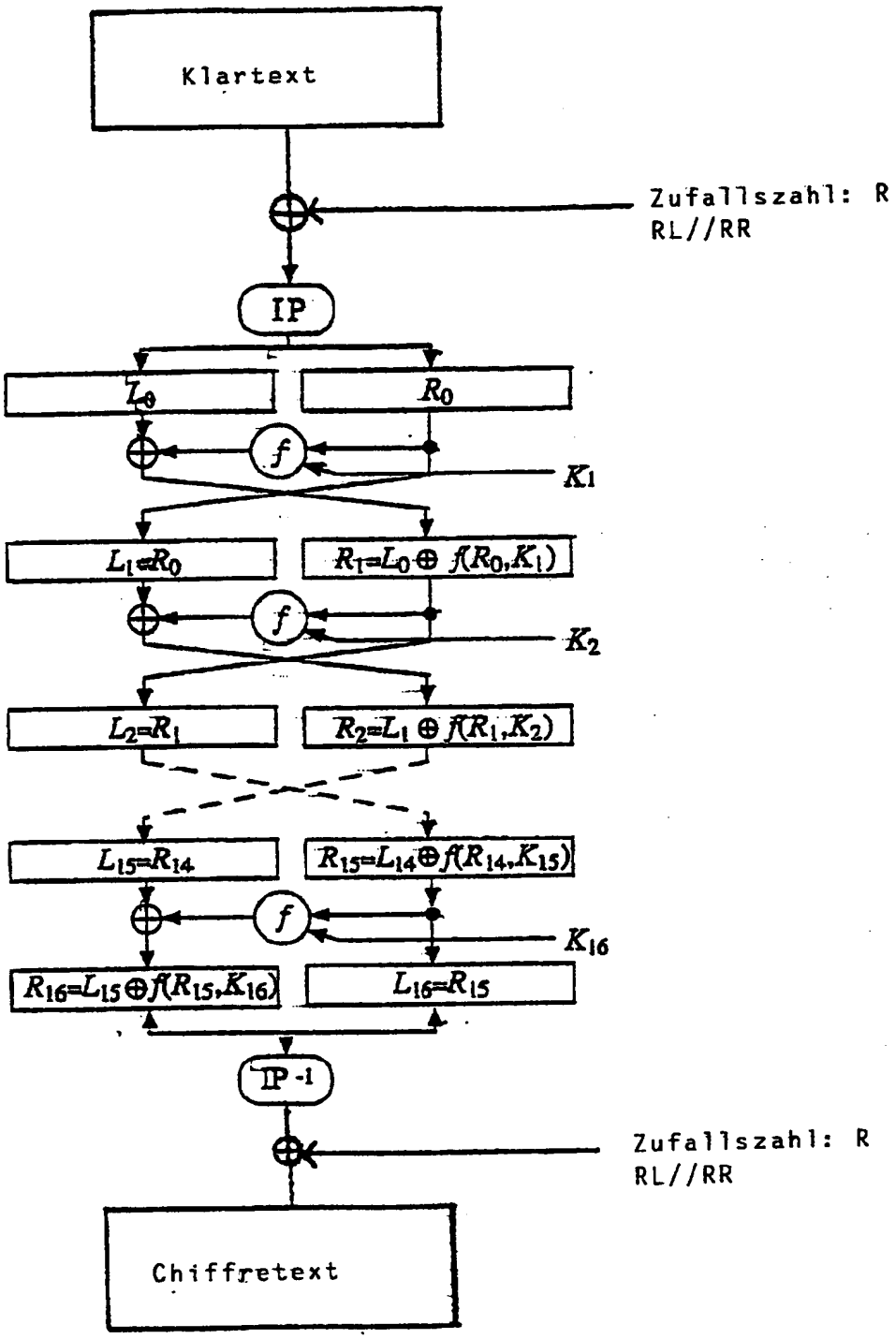
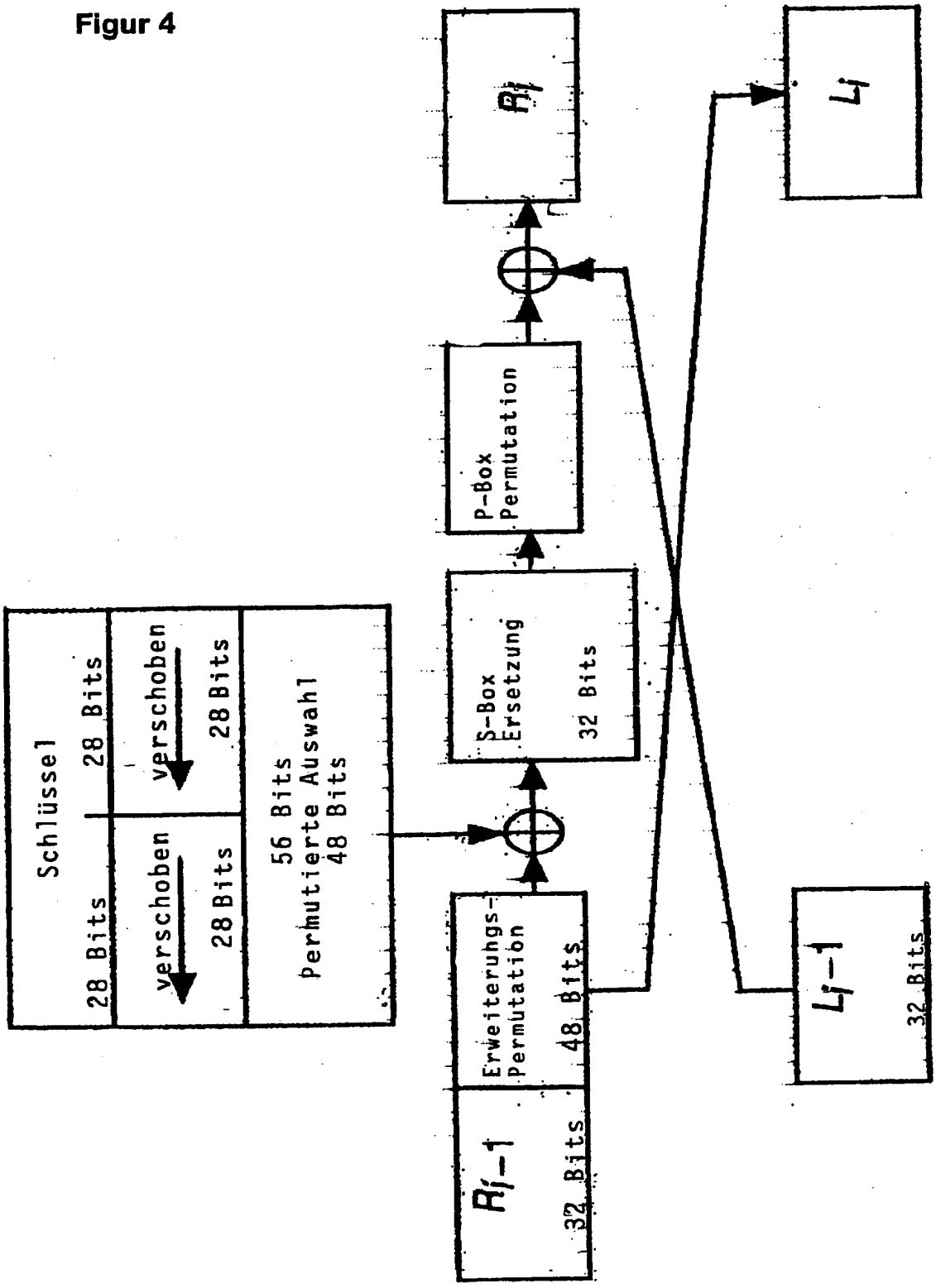


Fig.2

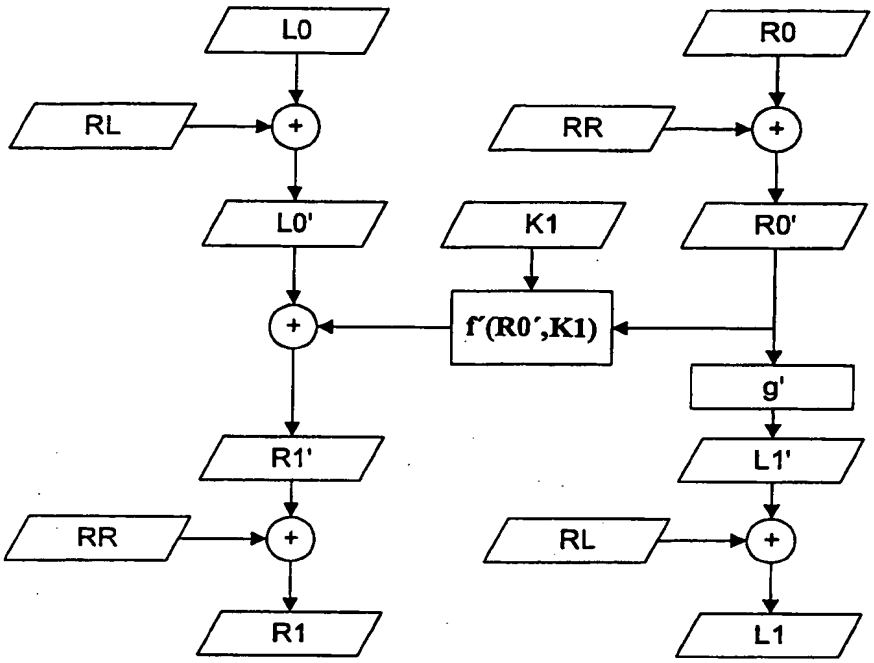

Klartext
Zufallszahl: R
RL//RR
IP
L_0
R_0
f
K_1
$L_1=R_0$
$R_1=L_0 \oplus f(R_0,K_1)$
K_2
$L_2=R_1$
$R_2=L_1 \oplus f(R_1,K_2)$
$L_{15}=R_{14}$
$R_{15}=L_{14} \oplus f(R_{14},K_{15})$
K_{16}
$R_{16}=L_{15} \oplus f(R_{15},K_{16})$
$L_{16}=R_{15}$
IP -1
Zufallszahl: R
RL//RR
Chiffretext

Figur 3

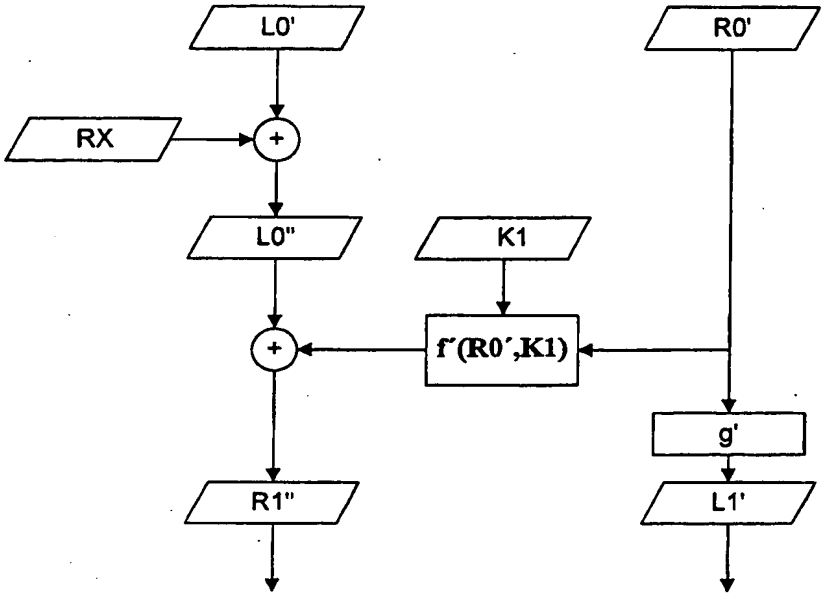
Figur 4



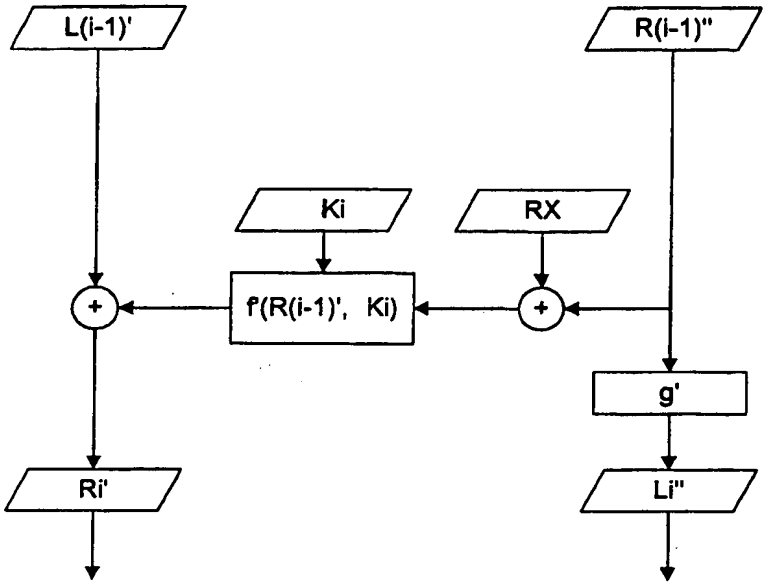
BERICHTIGTES BLATT (REGEL 91)
ISA/EP



Figur 5



Figur 6



Figur 7

INTERNATIONAL SEARCH REPORT

Interr ıal Application No
PCT/DE 00/02518

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	EP 0 981 223 A (TOKYO SHIBAURA ELECTRIC CO) 23 February 2000 (2000-02-23) abstract; figure 4 column 8, line 47 -column 15, line 32; figures 11,12,14,15	1-4
A	---	5,6
P,X	FR 2 785 477 A (GEMPLUS SOCIÉTÉ EN COMMANDITE PAR ACTIONS) 5 May 2000 (2000-05-05) page 14 -page 24; figures 3,4,8,10,12	1-4
A	---	5,6
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 December 2000	27/12/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Carnerero Álvaro, F

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interr: al Application No
PCT/DE 00/02518

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KOCHER P ET AL: "DIFFERENTIAL POWER ANALYSIS" 19TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. SANTA BARBARA, CA, AUG. 15 - 19, 1999. PROCEEDINGS,BERLIN: SPRINGER,DE, 1999, pages 388-397, XP000863414 ISBN: 3-540-66347-9 the whole document	1-6

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interr al Application No
PCT/DE 00/02518

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0981223 A	23-02-2000	JP 2000066585 A	03-03-2000
FR 2785477 A	05-05-2000	AU 6348699 A	22-05-2000
		WO 0027068 A	11-05-2000

INTERNATIONALER RECHERCHENBERICHT

Interr. ales Aktenzeichen
PCT/DE 00/02518

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/06

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, INSPEC, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
P,X	EP 0 981 223 A (TOKYO SHIBAURA ELECTRIC CO) 23. Februar 2000 (2000-02-23) Zusammenfassung; Abbildung 4 Spalte 8, Zeile 47 -Spalte 15, Zeile 32; Abbildungen 11,12,14,15	1-4
A	---	5,6
P,X	FR 2 785 477 A (GEMPLUS SOCIÉTÉ EN COMMANDITE PAR ACTIONS) 5. Mai 2000 (2000-05-05) Seite 14 -Seite 24; Abbildungen 3,4,8,10,12	1-4
A	---	5,6
	-/--	

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
11. Dezember 2000	27/12/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Carnerero Álvaro, F

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Interr. .ales Aktenzeichen
PCT/DE 00/02518

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	KOCHER P ET AL: "DIFFERENTIAL POWER ANALYSIS" 19TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. SANTA BARBARA, CA, AUG. 15 - 19, 1999. PROCEEDINGS,BERLIN: SPRINGER,DE, 1999, Seiten 388-397, XP000863414 ISBN: 3-540-66347-9 das ganze Dokument	1-6

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Intern. ...les Aktenzeichen
PCT/DE 00/02518

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0981223 A	23-02-2000	JP 2000066585 A	03-03-2000
FR 2785477 A	05-05-2000	AU 6348699 A	22-05-2000
		WO 0027068 A	11-05-2000